

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-261483

(43)Date of publication of application : 22.09.2000

(51)Int.Cl.

H04L 12/46

H04L 12/28

G06F 13/00

H04L 12/24

H04L 12/26

H04L 12/56

(21)Application number : 11-061185

(71)Applicant : HITACHI LTD

(22)Date of filing : 09.03.1999

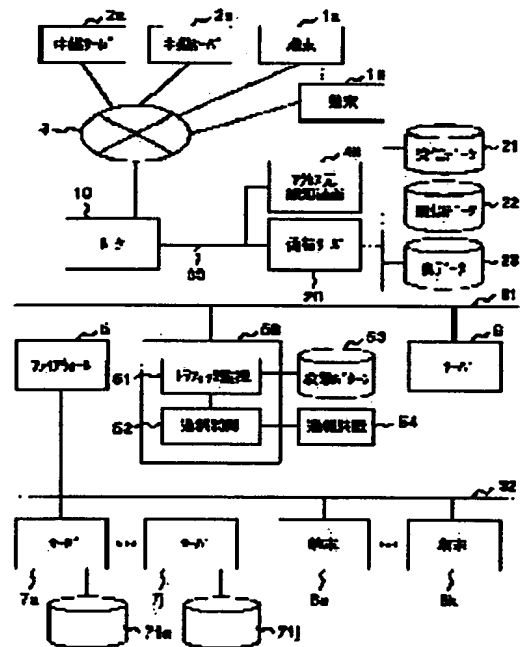
(72)Inventor : IDEMOTO MANABU

(54) NETWORK MONITORING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a network monitoring system where an illegal access from an external network to an in-enterprise information network can be detected and a transmission source of an illegal packet can be retrieved.

SOLUTION: The network monitoring system is provided with a traffic monitoring device 50 that monitors traffic of a packet passing through a router 10 and received from an external network 3 and informs the router about identification information of an illegal packet at the time of detecting the illegal packet and with a disguised server 20 that gives a false reply to a sender of the illegal packet. The router 10 identifies the illegal packet coming from the external network and transfers the illegal packet to the disguised server based on the identification information of the illegal packet informed from the monitoring device.



LEGAL STATUS

[Date of request for examination]

26.03.2003

BEST AVAILABLE COPY

(11)特許出願公開番号
特開2000-261483
(P2000-261483A)

(43)公開日 平成12年9月22日(2000.9.22)

(51)Int.Cl. ¹	識別記号	F I	デマコト ¹ (参考)
H 0 4 L 12/46		H 0 4 L 11/00	3 1 0 C 5 B 0 8 9
12/28		G 0 6 F 13/00	3 5 1 Z 5 K 0 3 0
G 0 6 F 13/00	3 5 1	H 0 4 L 11/08	5 K 0 3 3
H 0 4 L 12/24		11/20	1 0 2 Z
12/26			

審査請求 未請求 請求項の数14 OL (全 13 頁) 最終頁に続く

(21)出願番号	特願平11-61185	(71)出願人	000005108 株式会社日立製作所 東京都千代田区神田駿河台四丁目6番地
(22)出願日	平成11年3月9日(1999.3.9)	(72)発明者	出本 学 東京都国分寺市東恋ヶ窪一丁目280番地 株式会社日立製作所中央研究所内
		(74)代理人	100061893 弁理士 高橋 明夫 (外1名) Fターム(参考) 5B089 GA11 GA21 GA31 GB02 HA01 JB15 JB22 KA17 KB13 MC08 5K030 GA15 HA08 HCD1 HC14 HD03 HD06 MA01 MB09 5K033 AA08 BA08 CCD1 DA01 DA06 DB12 DB18 DB20 EA07 EC03

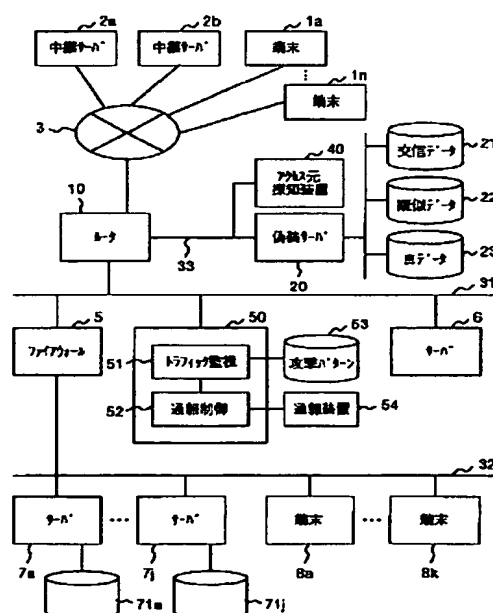
(54)【発明の名称】 ネットワーク監視システム

(57)【要約】

【課題】 外部ネットワークから企業内情報ネットワークへの不正アクセスを検出し、不正パケットの送信元探知を可能とするネットワーク監視システムを提供する。

【解決手段】 ルータ１０を通過する外部ネットワーク３からの流入パケットのトラフィックを監視し、不正トラフィックを検出した時、上記ルータ装置宛に不正パケットの識別情報を通知するトラフィック監視装置５０と、不正パケットの送信元に偽の応答をする偽装サーバ２０とを有し、上記ルータ１０が、監視装置から通知された上記不正パケットの識別情報に基づいて、外部ネットワークから流入する不正パケットを識別し、偽装サーバに転送する。

1



【特許請求の範囲】

【請求項1】外部ネットワークから、該外部ネットワークにルータを介して接続された内部情報ネットワークへの不正なアクセスを監視するネットワーク監視システムにおいて、

外部ネットワークから上記ルータを通過して流入するパケットのトラフィックを監視し、上記内部情報ネットワークを不正にアクセスするパケットを検出した時、上記ルータ装置宛に不正パケットの識別情報を示す制御パケットを送信するトラフィック監視装置と、

受信パケットにตอบสนองして、該パケットの送信元に、意図的な情報を含む応答パケットを送信する偽装サーバとを有し、

上記ルータが、監視装置からの上記制御パケットの受信にตอบสนองして、上記不正パケットの識別情報を記憶するための手段を備え、上記外部ネットワークから受信されたパケットの中から上記識別情報に基づいて不正パケットを識別し、上記偽装サーバに転送することを特徴とするネットワーク監視システム。

【請求項2】前記ルータが、前記外部ネットワークに接続された第1インタフェース回路と、前記内部情報ネットワークに接続された第2インタフェース回路と、前記偽装サーバに接続された第3のインタフェース回路とを有し、前記不正パケットを上記第3インタフェース回路に送出することを特徴とする請求項1に記載のネットワーク監視システム。

【請求項3】前記内部情報ネットワークが、内部情報サービス用の少なくとも1つのサーバを収容した内部セグメントと、前記ルータに接続された外部バリア・セグメントと、上記内部セグメントと上記外部バリア・セグメントとの間に接続され、上記外部バリア・セグメントから上記内部セグメントへの流入パケットを制限するためのファイアウォール装置とからなり、

前記トラフィック監視装置が、上記外部バリア・セグメントに接続され、上記外部バリア・セグメント上を流れるパケットのトラフィックを監視することを特徴とする請求項1に記載のネットワーク監視システム。

【請求項4】前記偽装サーバが、前記外部バリア・セグメントに接続され、前記ルータが、前記不正パケットの宛先アドレスを上記偽装サーバを示すアドレスに変更した後、上記外部バリア・セグメントに送出することを特徴とする請求項3に記載のネットワーク監視システム。

【請求項5】前記偽装サーバに付随して、該偽装サーバが受信する不正パケットの送信元を逆探知するための通信動作を行う送信元探知装置を備えたことを特徴とする請求項1～請求項4の何れかに記載のネットワーク監視システム。

【請求項6】外部ネットワークから、該外部ネットワークにルータを介して接続された内部情報ネットワークへの不正なアクセスを監視するネットワーク監視システム

において、

上記外部ネットワークから上記ルータを通過して流入するパケットのトラフィックを監視し、予め記憶された不正アクセスに特有の特徴をもつトラフィックを検出した時、該トラフィックに属した不正パケットの識別情報を含む制御パケットを生成して、上記ルータ装置宛に送信するトラフィック監視装置と、

受信パケットにตอบสนองして、該パケットの送信元に、意図的な情報を含む応答パケットを送信する偽装サーバとからなり、

上記ルータが、不正パケットの識別情報と出力回線との対応関係を記憶するためのフィルタリングテーブル手段と、受信パケットに含まれる宛先アドレスと出力回線との対応関係を記憶するためのルーティンテーブルと、上記監視装置から受信した制御パケットに応じて上記フィルタリングテーブルの内容を更新するための手段と、上記フィルタリングテーブルに基づいて、上記外部ネットワークからの受信パケットが不正パケットか否かを判定し、不正パケットは上記偽装サーバが接続された出力回線に転送し、正常パケットは上記ルーティンテーブルに基づいてルーティング処理するための手段とを備えたことを特徴とするネットワーク監視システム。

【請求項7】前記ルータが、前記偽装サーバに専用のインタフェース回路を有し、前記各不正パケットを上記偽装サーバに専用のインタフェース回路の出力することを特徴とする請求項6に記載のネットワーク監視システム。

【請求項8】前記内部情報ネットワークが、内部情報サービス用の少なくとも1つのサーバを収容した内部セグメントと、前記ルータに接続された外部バリア・セグメントと、上記内部セグメントと上記外部バリア・セグメントとの間に接続され、上記外部バリア・セグメントから上記内部セグメントへの流入パケットを制限するためのファイアウォール装置とからなり、

前記トラフィック監視装置が、上記外部バリア・セグメントに接続され、上記外部バリア・セグメント上を流れるパケットのトラフィックを監視することを特徴とする請求項6に記載のネットワーク監視システム。

【請求項9】前記偽装サーバが、前記内部情報ネットワークの一部を構成し、前記ルータが、前記各不正パケットの宛先アドレスを上記偽装サーバ宛のアドレスに変換した後、上記内部情報ネットワークが接続されたインタフェース回路に出力することを特徴とする請求項6または請求項8に記載のネットワーク監視システム。

【請求項10】前記偽装サーバに付随して、該偽装サーバが受信する不正パケットの送信元を逆探知するための通信動作を行う送信元探知装置を備えたことを特徴とする請求項6～請求項9の何れかに記載のネットワーク監視システム。

【請求項11】外部ネットワークから、該外部ネットワ

ークにルータを介して接続された内部情報ネットワークへの不正なアクセスを監視するネットワーク監視システムにおいて、

上記内部情報ネットワークが、内部情報サービス用の少なくとも1つのサーバを収容した内部セグメントと、前記ルータに接続された外部バリア・セグメントと、上記内部セグメントと上記外部バリア・セグメントとの間に接続され、上記外部バリア・セグメントから上記内部セグメントへの流入バケットを制限するためのファイアウォール装置と、外部ネットワークから上記外部バリア・セグメントに流入するバケットのトラフィックを監視し、上記内部情報ネットワークを不正にアクセスするバケットを検出した時、上記ファイアウォール装置宛に不正バケットの識別情報を示す制御バケットを送信するトラフィック監視装置と、上記ファイアウォール装置から転送された受信バケットに回答して、該バケットの送信元に、意図的な情報を含む応答バケットを送信する偽装サーバとを有し、

上記ファイアウォール装置が、上記監視装置からの受信した制御バケットに基づいて、上記不正バケットの識別情報を記憶しておき、上記外部ネットワークから受信されたバケットの中から上記識別情報に基づいて不正バケットを識別し、上記偽装サーバに転送することを特徴とするネットワーク監視システム。

【請求項12】前記偽装サーバに付随して、該偽装サーバが受信する不正バケットの送信元を逆探知するための通信動作を行う送信元探知装置を備えたことを特徴とする請求項11に記載のネットワーク監視システム。

【請求項13】外部ネットワークと内部ネットワークとの間に配置されたルータと、上記ルータを通過する上記外部ネットワークからの流入バケットのトラフィックを監視することによって、上記内部ネットワークを不正にアクセスする不正バケットを検出するためのトラフィック監視装置と、上記外部ネットワークと内部ネットワークとの間において上記ルータから不正バケットを受信し、該不正バケットの送信元に応答バケットを送信するサーバとを有し、

上記トラフィック監視装置が、上記内部ネットワークを不正にアクセスする不正バケットが検出された場合に、上記ルータに対して、該不正バケットのヘッダ情報で識別されるその後の特定の受信バケットを上記サーバに転送させるための制御情報を通知するための手段を有し、上記サーバが、上記内部ネットワークに接続された他のサーバが保持するデータの一部、または上記他のサーバとは異なるデータに基づいて、上記応答バケットを生成することを特徴とするネットワークシステム。

【請求項14】前記サーバが受信する不正バケットを監視し、該不正バケットの送信元を逆探知するための手段を有することを特徴とする請求項13に記載のネットワークシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワーク監視システムに関し、更に詳しくは、外部の通信ネットワークから企業内情報ネットワークへの不正アクセスに対処するための監視システムに関する。

【0002】

【従来の技術】インターネット等の外部通信ネットワークと企業内ネットワークとを接続する場合、外部から企業内情報システムへの不正侵入の防止手段として、ファイアウォール装置が知られている。ファイアウォールは、外部ネットワークからアクセスできる外部バリア・セグメントと、企業内情報ネットワークを構成する各種のサーバおよびユーザ端末が接続される内部セグメントとの間に位置し、外部から到着する不正なバケットを識別して、内部セグメントへの侵入を阻止する。

【0003】ファイアウォールの機能については、例えば、日経コミュニケーション、1996年7月1日、第68頁～第83頁に記載されているように、幾つかの方式が知られており、例えば、TCP/IPレイヤでアクセス制御するバケット・フィルタリング方式では、TCP/IPバケットの送信元アドレスと、宛先アドレスと、ポート番号とをチェックすることによって、バケットを通過させるか否かを判断している。上記ポート番号は、TCP/IPアプリケーション毎に予め決まった値となっており、予め登録された番号以外のポート番号をもったバケットは、ファイアウォールにおいて通過を拒否される。

【0004】また、企業内情報システムに対する不正侵入を監視するツールとして、例えば、日経オープンシステム、1998年8月（No.65）第130頁～第132頁には、ネットワーク上を流れるバケットのトラフィックを監視し、予め用意されている不正アクセスに特徴的なトラフィックパターン（攻撃パターン）と比較することによって、不審なトラフィックを検出する監視ツールが記載されている。上記監視ツールによって不審なトラフィックが検知されると、例えば、アラートの表示、コネクションの切断、重要ログ情報の保存等の措置がとられる。

【0005】

【発明が解決しようとする課題】企業内情報ネットワークへの侵入を図る不正ユーザが、外部ネットワークに接続された中継サーバを介して、企業内情報ネットワーク（以下、内部ネットワークと言う）をアクセスした場合、内部ネットワークからは、上記中継サーバが不正バケットの送信元（アクセス元）に見えるため、不正ユーザの操作する端末装置が隠蔽されてしまう。外部ネットワークから内部ネットワークへの不正侵入を検出した時点で、もし、該当コネクションを直ちに切断した場合、企業内情報の外部への漏洩やファイル情報の破壊等、そ

の後の被害を防止することができる。しかしながら、コネクションの切断によって不正パケットが途絶した状況下では、上記不正ユーザが操作する送信元端末の逆探知が困難となる。逆に、上記不正アクセスの中継点を含むパケットの侵入経路を逆探知できる迄、上記不正コネクションの切断を遅らせた場合は、外部に漏洩する情報量が増え、不正アクセスによって情報ファイルが破壊される危険性が增大するという問題がある。

【0006】重要な企業内情報の漏洩を防止し、不正アクセスの記録を残すことによって、不正端末の特定作業を支援するための従来技術の1つとして、例えば、特開平09-266475号公報では、ネットワークに接続された複数の端末装置の宛先アドレスを管理するアドレステーブルを備え、ネットワーク端末からの宛先アドレス問合せメッセージに回答して宛先アドレス通知メッセージを回答するアドレス管理サーバ、例えば、DNS(Domain Name System)や、ATM網のLECS(LAN Emulation Configuration Server)等のサーバに、問い合わせメッセージの送信元を識別するための認証手段を設けておき、不正ユーザからの問い合わせに対しては、上記ネットワークに接続された侵入対策用端末のアドレスを通知するようにしている。上記侵入対策用端末は、不正ユーザがアクセスしたいデータファイルは持っていないが、通信プロトコルの規定に従って不正ユーザと通信する機能と、不正ユーザからの受信パケットの内容を記録するための機能を備えており、不正ユーザからの要求に対して「該当情報なし」と回答しながら、不正ユーザとの通信期間中に受信パケットの内容を記録し、要求元アドレスの割り出しに必要な情報を収集するようになっている。

【0007】しかしながら、上記公開公報に示された従来技術は、端末からの宛先アドレスに回答するDNSやLECS等のサーバにおいて、受信メッセージの送信元アドレスから不正な問い合わせを検出するものであり、宛先アドレスの問い合わせを行うことなく企業内情報ネットワークに不正侵入を企てる端末ユーザに対しては有効ではない。また、上記従来技術では、侵入対策用端末が、不正ユーザからの情報要求に対して「該当情報なし」を回答するのみであるから、不正ユーザが宛先装置に不審を抱き、要求元の割り出しに必要な十分なデータを入手する前に、あるいは送信元の逆探知に成功する前に、通信が切断される可能性がある。

【0008】本発明の目的は、外部ネットワークから企業内情報ネットワークへの不正侵入を検知し、企業内の重要な情報を漏洩することなく、不正ユーザの逆探知に必要な通信保持あるいはデータ収集が可能なネットワーク監視システムおよびネットワークシステムを提供することにある。

【0009】

【課題を解決するための手段】上記課題を解決するため

に、本発明では、外部ネットワークから該外部ネットワークにルータを介して接続された内部情報ネットワークへの不正なアクセスを監視するネットワーク監視システムにおいて、外部ネットワークから上記ルータを通過して流入するパケットのトラフィックを監視し、上記内部情報ネットワークを不正にアクセスするパケットを検出した時、上記ルータ装置宛に不正パケットの識別情報を示す制御パケットを送信するトラフィック監視装置と、受信パケットに回答して、該パケットの送信元に意図的な情報を含む応答パケットを送信するサーバとを有し、上記ルータが、監視装置から受信した上記制御パケットに回答して、上記不正パケットの識別情報を記憶するための手段を備え、上記外部ネットワークから流入する受信パケットの中から上記識別情報に基づいて不正パケットを識別し、上記サーバに転送することを特徴とする。

【0010】尚、ここで言う意図的な情報は、例えば、擬似データファイルに予め用意された偽情報や、真の情報処理結果を改変して得られた疑似情報の他に、外部に漏洩しても問題のない真の情報をも含むものであって、監視システム側で不正アクセスが検知済みであることをユーザに悟られることなく、不正ユーザとの交信を持続するために意識的に提供される情報を意味している。本明細書では、不正パケットの送信元に対して、真のサーバに代わって、このような意図的な情報を含む応答パケットを送信するサーバを擬似サーバと言う。

【0011】本発明の1つの実施形態では、上記ルータが、外部ネットワークに接続された第1インタフェース回路と、内部情報ネットワークに接続された第2インタフェース回路と、偽装サーバに接続された第3インタフェース回路とを有し、不正パケットを上記第3インタフェース回路に送出することを特徴としている。上記第3インタフェースを偽装サーバに専用のインタフェースとすれば、ルータで受信パケットの宛先アドレスを書き替えることなく、不正パケットを偽装サーバに供給できる。

【0012】上記内部情報ネットワークは、例えば、内部情報サービス用の少なくとも1つのサーバを収容した内部セグメントと、上記ルータに接続された外部バリア・セグメントと、上記内部セグメントと上記外部バリア・セグメントとの間に接続され、外部バリア・セグメントから内部セグメントへの流入パケットを制限するためのファイアウォール装置とを備えた構成とする。内部情報ネットワークが、このようにファイアウォール装置を備えた構成となっている場合、上記外部バリア・セグメントにトラフィック監視装置を接続し、上記ルータから上記外部バリア・セグメントに出力されたパケットのトラフィックを監視させればよい。尚、本発明において、上述した偽装サーバは、必ずしもルータに直結する必要はなく、例えば、上記外部バリア・セグメントに接続してもよい。この場合、ルータにアドレス変換機能をもた

せ、不正パケットについては、宛先アドレスを上記偽装サーバ宛のアドレスに変更した後、上記外部バリア・セグメントに送出する。

【0013】本発明の好ましい実施形態では、ネットワーク監視システムが、上記偽装サーバに付随して、該偽装サーバが受信する不正パケットの送信元を逆探知するための通信動作を行う送信元探知装置を備えるたことを特徴とする。本発明によれば、不正ユーザからの要求に応答して、偽装サーバが要求元に偽情報を送信するようになっているため、不正ユーザを欺き、偽装サーバと不正ユーザとの間の通信を比較的長時間にわたって継続させることが可能となる。従って、不正ユーザが偽装サーバと通信中に、上記探知装置から不正パケットの中継経路を逆方向に辿って、送信元の端末を逆探知することが可能となる。また、偽装サーバと不正ユーザとが通信中に、偽装サーバが受信した不正パケットの内容、あるいは偽装サーバから不正ユーザに送信した応答パケットの内容等、不正アクセスの証拠となるデータを保存しておくことによって、これらの証拠データを不正ユーザの追跡や新たな不正行為の予防に利用できる。上記証拠データの保存機能は、上述した偽装サーバまたは探知装置に持たせればよい。

【0014】本発明のネットワーク監視システムにおいて、内部情報ネットワークと外部ネットワークとを接続するルータは、例えば、不正パケットの識別情報と出力回線との対応関係を記憶するためのフィルタリングテーブル手段と、受信パケットに含まれる宛先アドレスと出力回線との対応関係を記憶するためのルーティンテーブルと、上記監視装置から受信した制御パケットに応じて上記フィルタリングテーブルの内容を更新するための手段と、上記フィルタリングテーブルに基づいて、上記外部ネットワークからの受信パケットが不正パケットか否かを判定し、不正パケットは上記偽装サーバが接続された出力回線に転送し、正常パケットは上記ルーティンテーブルに基づいてルーティング処理するための手段とを備えることを特徴とする。

【0015】偽装サーバが、内部情報ネットワークの一部を構成している場合、上記ルータで、各不正パケットの宛先アドレスを上記偽装サーバ宛のアドレスに変換した後、上記内部情報ネットワークに出力する必要がある。この場合、アドレス変換に必要な不正パケット識別情報と偽装サーバアドレスとの対応関係は、上記フィルタリングテーブル手段から得ることができる。

【0016】本発明において、上述した偽装サーバへの不正パケットの転送機能は、上記ルータの代りに、ファイアウォール装置で行うようにしてもよい。ファイアウォールは、特定のパケットのみを内部セグメントに転送する一種のルータ機能を備えているため、トラフィック監視装置で検出した不正パケットの識別情報をファイアウォールに通知すれば、その後には到着する不正パケット

をファイアウォールから偽装サーバに転送することも可能である。この場合、ファイアウォールが備えるインタフェース回路の1つに偽装サーバを接続しておけば、宛先アドレスを変換することなく、不正パケットを偽装サーバに供給できる。

【0017】

【発明の実施の形態】以下、本発明の実施例を図面を参照して説明する。図1は、本発明によるネットワーク監視システムの1実施例を示すブロック図である。端末装置1a～1nと中継サーバ2a～2bは外部ネットワーク3に接続され、企業内情報ネットワークの外部バリア・セグメント31が、ルータ10を介して、上記外部ネットワーク3に結合されている。また、上記ルータ10には、信号線33を介して、後述する偽装サーバ20と、不正パケットの送信元（アクセス元）探知装置40とが接続されている。

【0018】上記外部バリア・セグメント31には、企業内情報ネットワークの内部セグメント（企業内LAN）32への不正侵入を防止するためのファイアウォール装置5と、企業内情報ネットワークへの不正アクセスを検知するための監視装置50と、例えばメールサーバのように、外部ネットワークのサーバと通信して情報を蓄積するためのサーバ6が接続されている。また、上記内部セグメント32には、各種の情報サービスを行うための複数のサーバ7（7a～7j）と、企業内ユーザが操作する複数の端末装置8（8a～8k）とが接続されている。

【0019】外部ネットワーク3からルータ10に到着するIPパケットは、例えば、図2に示すように、TCPパケット320とIPヘッダ330とからなる。上記TCPパケット320は、ユーザ情報が設定される可変長の情報部300とTCPヘッダ部310とからなり、TCPヘッダ部310は、送信元ポート番号311、宛先ポート番号312、その他のヘッダ情報を含む。また、IPヘッダ330は、送信元IPアドレス331、宛先IPアドレス332、プロトコル識別子333、その他のヘッダ情報を含んでいる。

【0020】図3は、ルータ10の構成を示す。ルータ10は、外部ネットワーク3との間でパケットを送受信するためのインタフェース回路11Aと、外部バリア・セグメント31との間でパケットを送受信するためのインタフェース回路11Bと、偽装サーバ20とアクセス元探知装置40が接続された信号線33との間でパケットを送受信するためのインタフェース回路11Cと、これらのインタフェース回路11（11A～11C）に内部バス30を介して結合され、インタフェース回路間のパケット転送を制御するルーティング制御装置12とからなる。

【0021】上記ルーティング制御装置12は、マイクロプロセッサによって構成され、パケットアドレスと出

10

20

30

40

50

力回線（インタフェース回路）との関係を定義したルーティング・テーブル140とフィルタリング・テーブル150とを記憶するためのメモリ14と、ルーティング制御に必要な各種のプログラムを格納したプログラムメモリ15とを備えている。

【0022】上記プログラムメモリ15には、後述するように、監視装置50から受信した制御パケットに従って、上記フィルタリングテーブル150を更新するためのテーブル管理モジュール110と、上記ルーティングテーブル140とフィルタリングテーブル150とを参照して、各インタフェース11（11A～11C）からの受信パケットを他の何れかのインタフェースに転送するルーティングモジュール120とを備えている。

【0023】ファイアウォール装置5は、通過許容パケットを識別するための定義情報を記憶したテーブルを備えており、ルータ10によって外部バリア・セグメント31に取り込まれた各IPパケットのヘッダ情報を上記定義情報に基づいてチェックする。ファイアウォール装置5は、例えば、使用プロトコル、送信元アドレス、ユーザ等によって識別された特定のパケットについて、内部セグメント32への通過を許容することによって、内部セグメント32に結合されたサーバ7a～7jへの不正なアクセスを防止する。

【0024】上記ファイアウォール装置5を潜り抜けて、企業内サーバ7a～7jを不正にアクセスしようとするユーザは、送信パケットのヘッダ情報から直接的に送信元端末が発覚するのを避けるため、1つあるいは複数の中継サーバを経由した形で、企業内情報システムのサーバ7をアクセスする場合がある。例えば、端末装置1aのユーザが、最終的に中継サーバ2aを経由して、不正パケットを送信した場合、パケットの送信元アドレスは、上記最終的な中継サーバ2aのアドレスとなっている。不正ユーザは、もし、ファイアウォール5を潜り抜けるためにパケットが備えるべき正しいヘッダ情報が判らない場合、ヘッダ情報の一部、例えば、プロトコル（サービス種類）を識別するための宛先ポート番号等を順次に変更しながら、目的のサーバから何らかの応答があるまで、次々と不正パケットを送信する。

【0025】監視装置50は、不正アクセスを試みた場合のパケットのトラフィックに現れる幾つかの特徴的なパターン（攻撃パターン）を記憶したデータファイル53と、外部バリア・セグメント31に流れるパケットのトラフィックを監視し、上記データファイルに登録された不正アクセスのパターンに類似した不正トラフィックを検知するためのトラフィック監視機能51と、不正トラフィックが検知された時、保守員に通知するために通報装置54に警報メッセージを出力する通報制御機能52を備えている。本発明では、不正トラフィックを検知した時、上記トラフィック監視機能51に、通報装置54の警報メッセージを出力すると共に、ルータ10に対

して、その後に到着する不正パケットを擬似サーバ20宛に転送させるための制御パケットを通知させる。

【0026】上記監視装置50は、具体的には、外部バリア・セグメント31との間でパケットを送受信するための通信インタフェースと、受信パケットから主要なヘッダ情報を抽出するための回路と、予め用意されたプログラムを実行するプロセッサとからなる。上述したトラフィック監視機能51は、受信パケットから抽出されたヘッダ情報を解析し、同一送信元から送信された一連のパケットについて、ヘッダ情報の時間的変化が示す特徴パターンを抽出し、上記データファイル53に登録してある攻撃パターンと照合するためのデータ処理プログラムによって実現される。

【0027】図4は、不正なトラフィック、すなわち、不正パケットが検出された場合に監視装置50からルータ10宛に送信される制御パケット500のフォーマットの1例を示す。上記制御パケット500は、パケットヘッダ510と、情報部520とからなる。パケットヘッダ510は、図2に示したIPパケットのヘッダ330と同一のフォーマットを有し、送信元アドレス511として監視装置50のアドレス、宛先アドレス512としてルータ10のアドレスを含む。また、情報部520は、ルータ10にパケット転送先の登録を指示するための制御命令フィールド521と、不正パケットの送信元IPアドレスを示すフィールド522と、不正パケットの現在の宛先IPアドレスを示すフィールド523と、不正パケットの転送先IPアドレスを示すフィールド524とからなり、上記転送先フィールド524には偽装サーバ20のアドレスが設定される。

【0028】図5は、ルータ10のルーティング・モジュール120が参照するルーティングテーブル140の構成の1例を示す。ルーティングテーブル140は、宛先IPアドレスの特定のビット部分を抽出するためのマスクとなるビットパターンあるいは位置情報が設定されるマスク141と、上記マスクによって抽出された部分的な宛先IPアドレスが設定される宛先IPアドレス・フィールド142と、受信パケットの送出先となる出力回線あるいはインタフェース回路の識別子を示す出力回線フィールド146とを有し、その他に必要に応じて、次サーバやプロトコル情報等を示すためのフィールド148を含む。

【0029】図6は、フィルタリングテーブル150の構成の1例を示す。フィルタリングテーブル150は、送信元IPアドレス・フィールド151と、宛先IPアドレス・フィールド152と、転送先IPアドレス・フィールド153と、出力回線フィールド154とからなる。上記フィルタリングテーブル150は、監視装置50から転送先登録を指令する制御パケット500を受信した時、ルータ10のテーブル管理モジュール110によって更新される。

【0030】図6に例示したエントリR100は、図4に例示した制御バケット500の受信に回答して登録されたものであり、フィールド151～153の内容は、上記制御バケット500の情報部にあるフィールド522～524の内容と対応している。本実施例の場合、出力回線フィールド154には、偽装サーバ20が接続されたインタフェース回路11Cの識別子が設定される。

【0031】図7は、ルーチングモジュール120の機能を示すプログラム・フローチャートを示す。上記ルーチングモジュール120は、インタフェース回路11から、制御バケット500以外の通常のIPバケットを受信した時に起動され、まず、受信バケットの送信元IPアドレス331と宛先IPアドレス332とに基づいて、フィルタリングテーブル150を検索する(ステップ121)。検索の結果、送信元IPアドレス151と宛先IPアドレス152との関係が上記受信バケットと一致するエントリまたはレコードが見つかった場合は、該当エントリの出力回線フィールド154が示すインタフェース回路に受信バケットを転送し(ステップ122～123)、このモジュールを終了する。本実施例の場合、フィルタリングテーブル150に該当エントリをもつ受信バケットは、偽装サーバ20に転送される。

【0032】上記受信バケットと対応するエントリがフィルタリングテーブル150になかった場合は、受信バケットの宛先IPアドレス332に基づいて、ルーティングテーブル140を検索する(ステップ124)。この場合、ルーティングテーブル140のマスクフィールド141が示すマスクパターンに従って、受信バケットの宛先IPアドレス332をマスクし、得られた部分的なアドレスビットがルーティングテーブル140の宛先IPアドレス142と一致するエントリ(目的エントリ)を探す。目的エントリが見つかった場合は、該エントリの出力回線フィールド146が示すインタフェース回路に受信バケットを送信し(ステップ125～126)、目的エントリが見つからなければ、受信バケットを廃棄し(ステップ127)、このプログラムモジュールを終了する。

【0033】図8は、偽装サーバ20の機能を示すプログラム・フローチャートである。偽装サーバ20は、ルータ10からIPバケットを受信すると、受信バケットの情報部300を解析し、受信バケットで使用しているアプリケーションの種類を識別する(ステップ201)。偽装サーバ20には、異なる複数種類のアプリケーションソフトに対応できるように、予め複数種類の処理ルーチン210(210A～210N)が用意されており、受信バケットは、それぞれが使用しているコマンド体系と対応したアプリケーションの処理ルーチン210に渡される(ステップ202A～202N)。受信バケットに対応したアプリケーションの処理ルーチンがなかった場合は、その他用の処理ルーチン203で受信バケ

ットを処理する。この場合は、例えば、ユーザ要求を実行できない旨を示す応答バケットが要求元に送信される。

【0034】上記アプリケーション別の処理ルーチン210は、基本的には、図9に示すように、受信バケットの情報部に含まれるコマンドを解析するステップ211と、ファイル名を解析して、使用ファイルを特定するステップ212と、コマンドを実行するステップ213と、コマンドの実行結果を示す応答メッセージを作成して、要求元に送信するステップ214と、不正ユーザとの通信内容をデータファイル21に記録するステップ215からなっている。

【0035】偽装サーバ20は、図1に示したように、不正ユーザとの通信記録を保存するためのデータファイル21と、不正ユーザを欺くために、ユーザからの要求に回答して偽の情報処理結果を通知するために用意された擬似データファイル22と、擬似データがない場合に企業内情報システムのサーバ7(7a～7j)から取り寄せた真のデータを格納するための新データファイル23とを備えており、企業内情報システムの各サーバ7が使用しているファイル名と上記2つのデータファイル22、23の関係を、例えば、図10に示すファイルテーブル24によって管理している。尚、企業にとって外部に漏洩しても影響のない機密性の低いデータファイルについては、真のデータをそのまま擬似データとして上記擬似データファイルに格納してもよい。

【0036】上記ファイルテーブル24は、サーバ7を示す識別子241と対応して、ファイル名242と、ディスク装置(データファイル22および23)におけるファイル名243と、データの真偽を示す属性情報244との関係を示している。上述したアプリケーション別の処理ルーチン210におけるファイル解析ステップ212では、上記ファイルテーブル24を参照することによって、各受信バケットに含まれるファイル名242と対応した擬似データファイル22内の偽ファイルを特定する。また、コマンド実行ステップ213では、上記偽ファイルに対してコマンドを実行する。

【0037】もし、偽ファイルが用意されていない場合は、サーバ識別子241が示す企業内サーバ7のデータファイル71(71a～71j)から、必要なデータをデータファイル23に転送した後、コマンドを実行する。この場合、得られた実行結果を所定のアルゴリズムで偽の実行結果に変換してから要求元に送信することによって、機密の漏洩を防止する。尚、真のデータを使用せざるを得ないコマンドの実行は、企業内サーバ7で行うようにしてもよい。この場合、例えば、偽装サーバ20が、送信元IPアドレスを偽装サーバ20のアドレスに一旦置換えた形で不正バケットを目的の企業内サーバ7に転送することによって、上記サーバ7が偽装サーバ20宛に回答バケットを送信するようにしておき、上記

応答パケットが示す真のコマンド実行結果を偽装サーバ20で偽情報に変換した後、不正ユーザに送信するようにすればよい。

【0038】上記実施例では、企業内情報ネットワークへの不正なアクセスを監視装置50で検知し、その後に到着する不正パケットを偽装サーバ20に転送することによって、偽装サーバ20から尤らしい情報、実は偽の情報、不正ユーザに偽情報に偽装して送っている。上記構成によれば、不正ユーザは、アクセス先から一見、尤らしい情報を受信できるため、アクセスに成功したものと判断して、その後も新たな要求パケットを次々と送信することになる。従って、偽装サーバ20からの応答動作によって、不正ユーザとの通信時間を引き延ばし、その間の通信記録をデータファイル21に残すことができる。

【0039】図1に示した構成によれば、信号線33を介して偽装サーバ20に転送される不正ユーザからの送信パケットは、偽装サーバに付随して上記信号線33に結合されたアクセス探知装置40で受信することができる。従って、偽装サーバ20が不正ユーザとの通信を引き延ばしている間に、探知装置40が、不正パケットの送信元アドレスで特定される中継サーバXに警報メッセージを送信し、中継サーバXが、不正パケットの上流側に位置した更に他の中継サーバに警報メッセージを送信する形式で、上記不正パケットの送信元端末を逆探知することが可能となる。

【0040】図1に示した実施例では、不正ユーザとの通信記録を偽装サーバ20のデータファイル21に残すようにしているが、不正ユーザと偽装サーバとの間の通信記録を探知装置40によって記憶するようにしてもよい。この場合、探知装置自身が行う不正ユーザの逆探知プロセス、または追跡結果を上記通信記録と共に残すことができるため、不正アクセスの証拠資料として利用しやすくなる。

【0041】また、上記実施例では、偽装サーバ20とアクセス探知装置40を信号線33を介してルータ10のインタフェース回路11Cに接続した構成となっているが、上記偽装サーバ20とアクセス探知装置40を外部バリア・セグメント31に接続してもよい。この場合は、図6に示したフィルタリングテーブル150の出力回線フィールド154に、上記外部バリア・セグメント31が接続されるインタフェース回路11Bの識別子を設定しておき、図7に示したルーティングモジュール120のフローチャートにおいて、ステップ123で、受信パケットの宛先IPアドレスを偽装サーバのアドレスに変換した後、パケット転送するようにすればよい。偽装サーバのアドレスは、ステップ121でフィルタリングテーブル150から検索した目的エントリの転送先IPアドレス・フィールド153から得られる。

【0042】次に、図11～図14を参照して本発明の第2実施例について説明する。第2実施例では、ルーテ

ィング・テーブル140を参照して、受信パケットの送信元アドレスもチェックすることによって、ルータ10に、或る程度のファイアウォール機能をもたせたことを特徴としている。

【0043】図11は、本実施例におけるルーティングテーブル140の1例を示す。ルーティングテーブル140の各エントリは、送信元のIPアドレスをマスクするためのマスクパターンを示すフィールド141と、上記マスクパターンでマスクされた部分的な送信元IPアドレスを示すフィールド142と、受信パケットの入力回線（インタフェース回路）の識別子を示すフィールド143と、宛先IPアドレスをマスクするためのマスクパターンを示すフィールド144と、上記マスクパターンでマスクされた部分的な宛先IPアドレスを示すフィールド145と、受信パケットの出力回線（インタフェース回路）の識別子を示すフィールド146と、属性フィールド147と、必要に応じてプロトコル等の他の項目データが設定されるフィールド148とからなる。

【0044】上記属性フィールド147は、そのエントリで定義された送信元と宛先との関係を満たす受信パケットについての処理区分を示しており、本実施例では、出力回線フィールド146で指定された出力回線への受信パケットの中継を“許可”するか、“禁止”するか、または、フィルタリングテーブル150が指定する出力回線に“転送”すべきかを示す区分コードが設定される。

【0045】図12は、上記第2実施例で使用されるフィルタリングテーブル150の1例を示す。本実施例では、フィルタリングテーブル150の各エントリは、上記ルーティングテーブルのフィールド141～145と同様の、送信元および宛先情報を示すためのフィールド161～165と、転送先のIPアドレスを示すフィールド166と、出力回線識別子を示すフィールド167とからなっている。上記転送先フィールド166には、偽装サーバ20のIPアドレスが設定され、出力回線フィールド167には、上記偽装サーバ20が接続されたインタフェース回路11Cの識別子が設定される。

【0046】図13は、本実施例において、監視装置50から図4に示す制御パケット500を受信した場合にルータ10が実行するテーブル管理モジュール110のプログラムフローチャートを示す。まず、ルーティングテーブル140を検索し（ステップ111）、制御パケット500の情報部520に含まれる送信元IPアドレス522と宛先IPアドレス523との関係を定義したエントリ（目的エントリ）が登録済みか否かを判定する（ステップ112）。もし、目的エントリが既に登録済みの場合は、属性フィールド147が“転送”となっているか否かを判定し（ステップ113）、既に“転送”となっていた場合は、このルーチンを終了する。

【0047】目的エントリの属性フィールドが“転送”

以外の場合は、その内容を“転送”を示すコードに変更（ステップ114）した後、フィルタリングテーブル150に、上記目的エントリと対応する新たなエントリを追加登録し（ステップ116）、このルーチンを終了する。ルーティングテーブル140に目的エントリが無かった場合は、受信した制御パケット500に従って新たなエントリを生成し、これをルーティングテーブルに追加登録（ステップ115）した後、ステップ116を実行する。例えば、図4に示した内容の制御パケット500を受信した時点で、ルーティングテーブル140には、図11に例示するように、送信元サーバXと宛先サーバYに関して、それぞれのセグメント間の関係を定義したエントリR201のみが登録されていた場合、これらのサーバのIPアドレスの関係を定義した新たなエントリR202を生成し、これをテーブルサーチにおいて上記エントリR201よりも優先する位置に登録する。

【0048】上記新たなエントリR202の入力回線フィールド143には、外部ネットワークと接続されたインタフェース回路11Aの識別子が設定され、出力回線フィールド146には初期値または無効データ、属性フィールド147には“転送”を示すコードが設定される。また、上記新たなエントリR202の送信元IPアドレスフィールド142および宛先IPアドレスフィールド145には、制御パケット500の送信元IPアドレスフィールド522および宛先IPアドレスフィールド523から得られたアドレスが設定され、それぞれと対応するマスクフィールド141、144には、マスク不要を示した状態となっている。

【0049】また、図12に例示するように、フィルタリングテーブル150には、サーバX、YのIPアドレスと、転送先アドレス（偽装サーバ20）と、出力回線との関係を定義した新たなレコードR102が追加される。本実施例の場合、偽装サーバ20がルータ10のインタフェース回路11Cに接続されているため、出力回線フィールド167には上記インタフェース回路11Cを示す識別子が設定される。

【0050】図14は、本実施例におけるルーチングモジュール120の処理動作を示すプログラムフローチャートを示す。インタフェース回路11からパケットを受け取ると、入力回線（インタフェース回路）の識別子と、受信パケットの送信元IPアドレス331と、宛先IPアドレス332とに基づいて、ルーティングテーブル140を検索する（ステップ131）。この場合、マスクパターンが指定されたエントリでは、上記送信元IPアドレス331と宛先IPアドレス332をマスクパターンに従ってマスクした上で、受信パケットに該当するエントリ（目的エントリ）を検索する。

【0051】検索の結果を判定し（ステップ132）、もし、目的エントリが見つからなければ無ければ、受信パケットを廃棄（ステップ133）して、このルーチン

を終了する。目的エントリが見つかった場合、目的エントリの属性フィールド147を判定し、属性フィールドが“廃棄”を示していた場合は（ステップ134）、パケットを廃棄して（ステップ133）、このルーチンを終了する。属性フィールドが“許可”を示していた場合は（ステップ135）、出力回線フィールド146で指定されたインタフェース回路に受信パケットを送出し（ステップ136）、このルーチンを終了する。上記属性フィールドが“転送”を示していた場合は、上記ルーティングテーブルの検索と同様に、フィルタリングテーブル150を検索し（ステップ137）、検索されたエントリの出力回線フィールド167が示すインタフェース回路に受信パケットを転送（ステップ138）した後、このルーチンを終了する。

【0052】尚、偽装サーバ20とアクセス元検知装置40を外部バリア・セグメント31に接続した場合は、上記フィルタリングテーブル150の出力回線フィールド167にインタフェース回路11Bの識別子を設定しておき、上記ステップ138で、受信パケットの宛先IPアドレス332を転送先IPアドレスフィールド524が示す偽装サーバ20のアドレスに変換した後、出力回線フィールド167が示す識別子に従って、インタフェース回路11Bに受信パケットを送出すればよい。

【0053】ファイアウォール装置は、ルータに類似した受信パケット処理機能をもっているため、上述した偽装サーバ20とアクセス元検知装置40を図1に示すファイアウォール装置5に接続し、監視装置50が送信した制御パケット500をファイアウォール5で受信し、ファイアウォール5が、その後には到着する不正パケットを偽装サーバ20に転送する構成としても良い。

【0054】

【発明の効果】以上の説明から明らかなように、本発明では、外部ネットワークから企業内ネットワークに不正にアクセスするパケットを不正アクセス・トラフィックが示す特徴に基づいて検知し、不正パケットを偽装サーバに転送し、偽装サーバから不正ユーザに意図的な情報を応答することによって、不正ユーザと偽装サーバとの間での通信を引き延ばすようにしている。従って、本発明によれば、不正ユーザが偽装サーバと通信している間に、不正パケットの経路を逆に辿って送信元を追跡し、不正ユーザ端末を逆探知するのに必要な時間を得ることができ、不正アクセスの抑制に効果がある。

【図面の簡単な説明】

【図1】本発明のネットワーク監視システムの1実施例をブロック構成図。

【図2】上記ネットワーク監視システムで使用されるパケットフォーマットの1例を示す図。

【図3】図1に示したルータ10の詳細を示すブロック図。

【図4】図1に示した監視装置50から送信される制御

10

20

30

40

50

17

パケットのフォーマットの1例を示す図。

【図5】ルータ10が備えるルーティングテーブル140の1実施例を示す図。

【図6】ルータ10が備えるフィルタリングテーブル150の1実施例を示す図。

【図7】ルータ10が備えるルーティングモジュールの1実施例を示すプログラム・フローチャート。

【図8】図1に示した偽装サーバ20の機能を示すプログラム・フローチャート。

【図9】図8における処理ルーチン210の詳細を示す10
プログラム・フローチャート。

【図10】上記偽装サーバ20が備えるファイルテーブル24の1例を示す図。

【図11】ルータ10が使用するルーティングテーブル140の他の実施例を示す図。

【図12】ルータ10が使用するフィルタリングテーブル150の他の実施例を示す図。

*

18

*【図13】ルータ10が備えるテーブル管理モジュール110の他の実施例を示すプログラム・フローチャート。

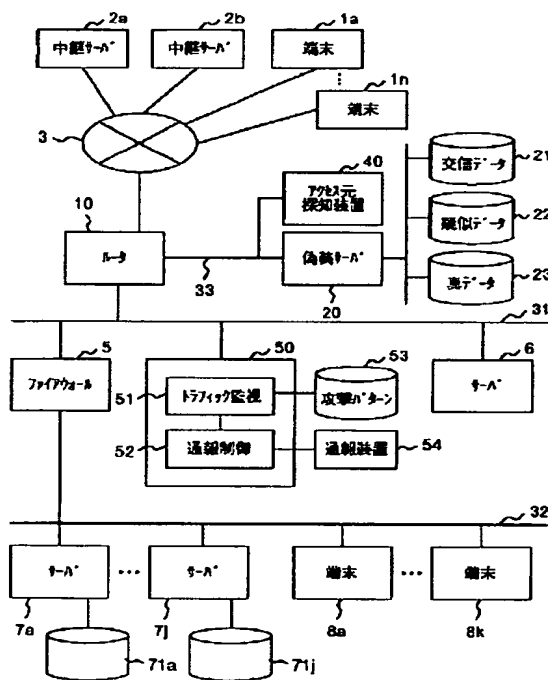
【図14】ルータ10が備えるルーティングモジュール120の他の実施例を示すプログラム・フローチャート。

【符号の説明】

1：外部の端末装置、2：中継サーバ、3：外部ネットワーク、5：ファイアウォール装置、7：サーバ、8：内部の端末装置、10：ルータ、11：インタフェース回路、12：ルーティング制御装置、20：偽装サーバ、22：擬似データファイル、40：アクセス元探知装置、50：ネットワーク監視装置、53：攻撃パターン記憶ファイル、110：テーブル管理モジュール、120：ルーティングモジュール、140：ルーティングテーブル、150：フィルタリングテーブル、500：制御パケット。

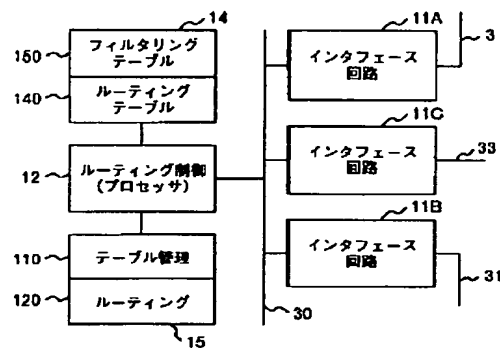
【図1】

図 1



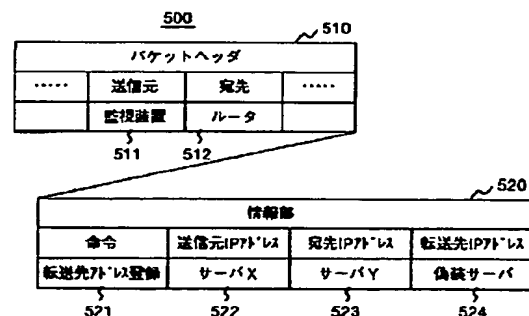
【図3】

図 3



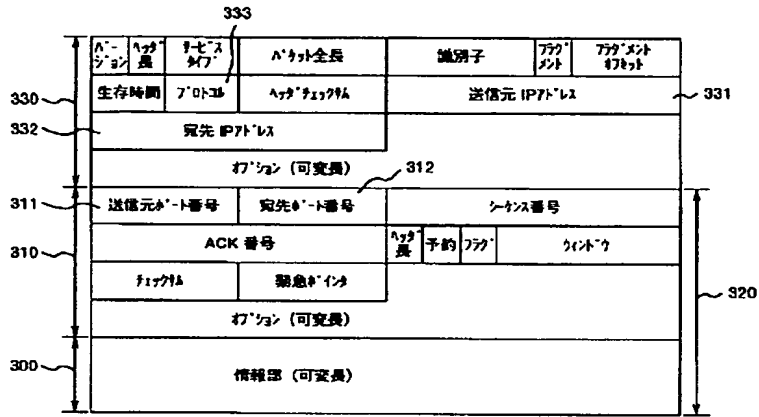
【図4】

図 4



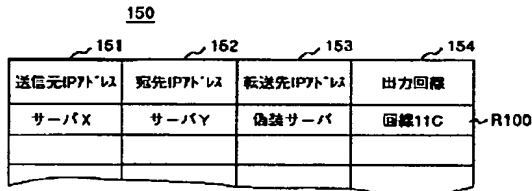
【図2】

図 2



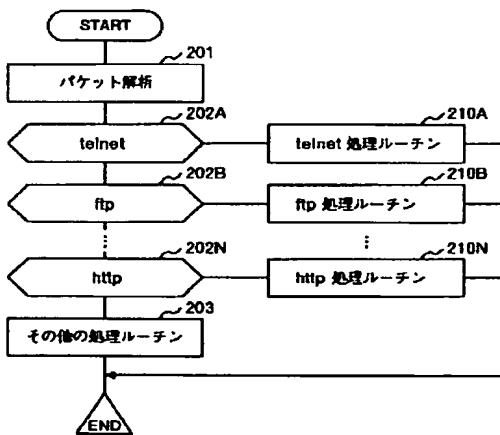
【図6】

図 6



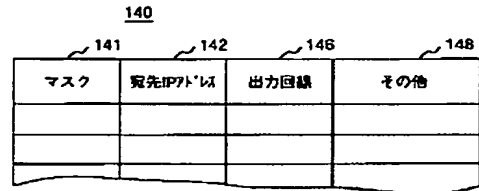
【図8】

図 8



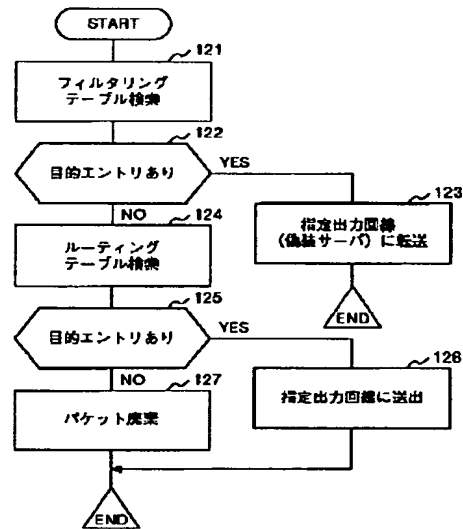
【図5】

図 5



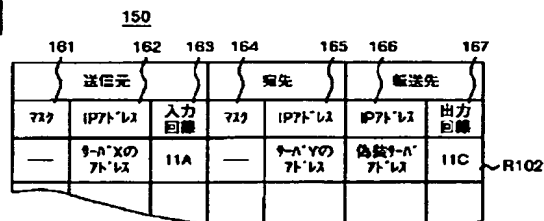
【図7】

図 7



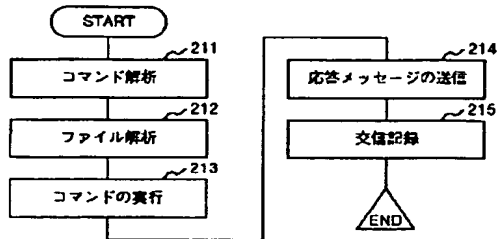
【図12】

図 1 2



【図9】

図 9



【図10】

図 10

24

サーバ	ファイル名	ディスク位置	属性 (真、偽)
XXXXX	/etc/passwd	/.../passwd. etc.	偽
⋮	⋮	⋮	⋮
XXXXX	/home/data	/.../131a/home/data	真
⋮	⋮	⋮	⋮

【図11】

図 11

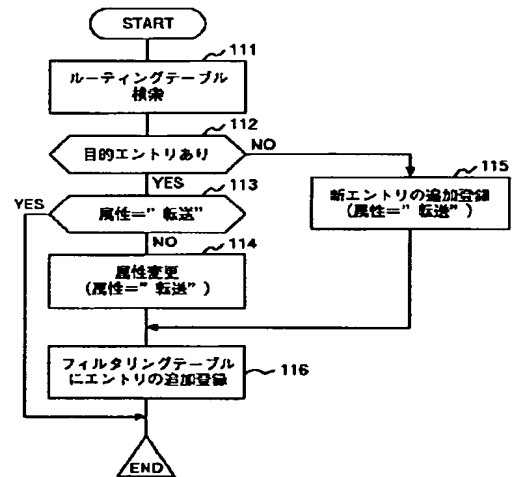
140

送信元			宛先			属性	その他
アドレス	IPアドレス	入力回線	アドレス	IPアドレス	出力回線		
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
—	サーバのアドレス	11A	—	サーバのアドレス	—	転送	XXXX
XXXX	サーバのアドレス	11A	XXXX	サーバのアドレス	11B	許可	XXXX

R202 R201

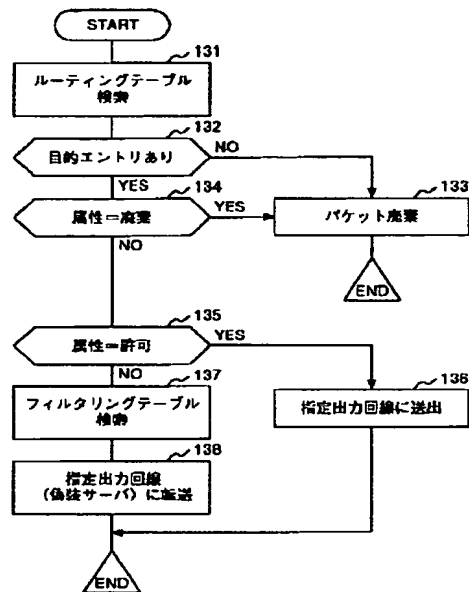
【図13】

図 13



【図 14】

図 14



フロントページの続き

(51)Int.Cl.⁷

H04L 12/56

識別記号

F I

テーマコード(参考)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.